CLAIMS

1. A privilege management system for managing service reception privileges of user devices;

wherein a user device which is a service reception entity holds a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer;

and wherein a service provider which is a service providing entity has a configuration for executing verification, by means of signature verification, of the group attribute certificate presented from said user device regarding whether or not there has been tampering, performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not service can be provided, based on said screening.

2. A privilege management system according to Claim 1, wherein said group attributes certificate is a certificate issued to a user device corresponding to a device or a user, under the conditions that mutual authentication is

established between a group attributes certificate issuing entity and the user device, and that the device or user to which the certificate is to be issued is following an issuance policy permitted by said service provider.

3. A privilege management system according to Claim 1, wherein the issuing processing for a new group attributes certificate is of a configuration carried out under the condition that verification is established at the group attributes certificate issuing entity regarding an already-issued group attributes certificate which the user device already holds.

4. A privilege management system according to Claim 1, wherein said service provider is of a configuration having a group information database wherein said group identifier and permitted service information for members belonging to the group are correlated, wherein said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device, and determining processing regarding whether or not service can be provided is executed.

5. A privilege management system according to Claim 1, wherein said service provider is of a configuration wherein

screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device, and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission.

6. A privilege management system according to Claim 1, wherein said service provider is of a configuration wherein screening regarding whether or not the object of service permission is executed for first group identification information obtained from a first group attribute certificate based on group definitions from said user device wherein devices are group members, and screening regarding whether or not the object of service permission is executed for second group identification information obtained from a second group attribute certificate based on group definitions from said user device wherein devices are group users, and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission.

7. A privilege management system according to Claim 1, wherein said user device is of a configuration including an end entity as a device for executing communication with said service provider, and a user identification device as an individual identification device;

wherein said group attribute certificate is issued individually to each of said end entity and user identification device, with issuing processing being carried out under the condition that mutual authentication has been established between the group attribute certificate issuing entity and said end entity or said user identification device.

8. A privilege management system according to Claim 1, of a configuration wherein said group attribute certificate is an attribute certificate issued by an attribute authority, and a group identifier is stored in an attribute information filed within the attribute certificate.

9. A privilege management system according to Claim 1, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein said service provider is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

10. An information processing device for executing data processing as service providing processing, comprising:

a data reception unit for receiving a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer; and

a group attribute certificate verification processing unit for executing verification, by means of signature verification, of the group attribute certificate regarding whether or not there has been tampering, performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not service can be provided, based on said screening.

11. An information processing device according to Claim 10, of a configuration further comprising a group information database wherein said group identifier and

permitted service information for members belonging to the group are correlated;

wherein said group attribute certificate verification processing unit searches said group information database based on the group identification information stored in said group attributes certificate presented by said user device, and executes determining processing regarding whether or not service can be provided.

12. An information processing device according to Claim 10, wherein said group attribute certificate verification processing unit is of a configuration wherein screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device, and determining processing regarding whether or not service can be provided is executed.

13. A privilege management method for managing service reception privileges of user devices, comprising:

as an execution step at a user device which is a service reception entity, a step for transmitting to a service provider which is a service providing entity a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer;

and, as an execution step at said service provider, a step for performing verification, by means of signature verification, of the group attribute certificate presented from said user device regarding whether or not there has been tampering, performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not service can be provided, based on said screening.

14. A privilege management method according to Claim 13, further comprising a group attribute certificate issuing processing step for issuing said group attributes certificate to a user device corresponding to a device or a user;

wherein said group attribute certificate issuing processing step is a processing step for issuing the group attribute certificate to a user device corresponding to a device or a user under the conditions that mutual authentication is established between a group attributes certificate issuing entity and the user device, and that the device or user to which the certificate is to be issued is following an issuance policy permitted by said service provider.

15. A privilege management method according to Claim 14, wherein said group attribute certificate issuing processing step includes a verification processing step regarding an already-issued group attributes certificate which the user device already holds, wherein issuing of a group attributes certificate is carried out under the condition that said verification is established.

16. A privilege management method according to Claim 13, wherein said service provider is of a configuration having a group information database wherein said group identifier and permitted service information for members belonging to the group are correlated, wherein said group information database is searched based on the group identification information stored in said group attributes certificate presented by said user device, and determining processing regarding whether or not service can be provided is executed.

17. A privilege management method according to Claim 13, wherein said service provider is of a configuration

wherein screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a plurality of different group definitions presented by said user device, and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission.

18. A privilege management method according to Claim 13, wherein at said service provider, screening regarding whether or not the object of service permission is executed for first group identification information obtained from a first group attribute certificate based on group definitions from said user device wherein devices are group members, and screening regarding whether or not the object of service permission is executed for second group identification information obtained from a second group attribute certificate based on group definitions from said user device wherein devices are group users, and determining processing regarding whether or not service can be provided is executed under the condition that all group identification sets are the object of service permission.

19. A privilege management method according to Claim 13, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein said service provider is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

20. An information processing method for an information processing device for executing data processing as service providing processing, said method comprising:

a certificate reception step for receiving from a service providing device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer, as an attribute certificate to be applied to service usage privilege confirmation processing; and

a group attribute certificate verification processing step for executing verification, by means of signature verification of the group attribute certificate, regarding whether or not there has been tampering, performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not service can be provided, based on said screening.

21. An information processing method according to Claim 20, said information processing device further comprising a group information database wherein said group identifier and permitted service information for members belonging to the group are correlated;

wherein said group attribute certificate verification processing step includes a step for searching said group information database based on the group identification information stored in said group attributes certificate presented by said user device, and executing determining processing regarding whether or not service can be provided.

22. An information processing method according to Claim 20, wherein said group attribute certificate verification processing step includes a step for executing screening regarding whether or not the object of service permission is executed for each of a plurality of sets of different group identification information obtained from a plurality of group attribute certificates based on a

plurality of different group definitions presented by said user device, and executing determining processing regarding whether or not service can be provided under the condition that all group identification sets are the object of service permission.

23. A computer program for effecting execution of privilege management processing for managing service reception privileges of user devices, said program comprising:

a certificate reception step for receiving from a service providing device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer, as an attribute certificate to be applied to service usage privilege confirmation processing; and

a group attribute certificate verification processing step for executing verification, by means of signature verification of the group attribute certificate, regarding whether or not there has been tampering, performing screening regarding whether or not this is a service-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not service can be provided, based on said screening.

24. An access privilege management system for executing access restrictions between communication devices having communication functions;

wherein an access requesting device stores, in storage means, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer;

and wherein an access requested device, which is the object of an access request from said access requesting device, executes verification, by means of signature verification, of the group attribute certificate presented from said access requesting device regarding whether or not there has been tampering, performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate, and executes determination regarding whether or not access can be permitted, based on said screening.

25. An access privilege management system according to

Claim 24, wherein said access requested device has a configuration for performing screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group, based on a group attribute certificate issued to the end entity which is an access executing device making up said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening.

26. An access privilege management system according to Claim 24, wherein said access requested device has a configuration for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group, based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening.

27. An access privilege management system according to Claim 24, of a configuration wherein said access requesting device and said access requested device have security chips with anti-tampering configurations, with mutual authentication being executed between the mutual security

chips, and wherein, under the condition that mutual authentication has been established, said access requested device executes signature verification of the group attribute certificate presented from said access requesting device, and screening regarding whether or not the device belongs to an access-permitted group.

28. An access privilege management system according to Claim 24, of a configuration wherein said access requested device receives from a device an issuing request for a group attribute certificate certifying that the device is an access-permitted group member;

and wherein, under the conditions that mutual authentication between devices has been established and that the group attribute certificate issue requesting device is following an issuance policy permitted by said access requested device, issues a group attribute certificate to a device corresponding to a device or a user, certifying that the device is an access-permitted group member.

29. An access privilege management system according to Claim 24, of a configuration wherein said access requested device receives from a device an issuing request for a group attribute certificate certifying that the device is an access-permitted group member;

and wherein, under the conditions that mutual authentication between devices has been established and that verification and screening is established for an already-issued group attribute certificate already held by the group attribute certificate issue requesting device, issues a group attribute certificate to a device corresponding to a device or a user, certifying that the device is an access-permitted group member.

30. An access privilege management system according to Claim 24, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein said access requesting device is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

31. A communication processing device for executing access restriction processing, comprising:

a reception unit for receiving, from an access requesting device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer; and

an access privilege determination processing unit for executing group attribute certificate verification processing functions, for executing verification, by means of signature verification, of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering, performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate, and executing determination regarding whether or not access can be permitted, based on said screening.

32. A communication processing device according to Claim 31, wherein said access privilege determination processing unit has a configuration for performing screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group, based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening.

33. A communication processing device according to Claim 31, wherein said access privilege determination processing unit has a configuration for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group, based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening.

34. A communication processing device according to Claim 31, comprising an encipherment processing unit for executing mutual authentication with said access requesting device;

wherein said access privilege determination processing unit has a configuration for, under the condition that mutual authentication has been established, executing signature verification of the group attribute certificate presented from said access requesting device, and screening regarding whether or not the device belongs to an access-permitted group.

35. A communication processing device according to

Claim 31, further comprising an attribute certificate generating unit for generating a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer.

36. A communication processing device according to Claim 31, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein said access privilege determination processing unit is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

37. An access privilege management method for executing access restrictions between communication devices having communication functions, said method comprising:

a step for an access requesting device to transmit to an access requested device, which is the object of an access request, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer;

a step for said access requested device to receive the group attribute certificate presented by said access requesting device;

a screening step for executing verification, by means of signature verification, of the group attribute certificate presented from said access requesting device regarding whether or not there has been tampering, and performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate;

and a step for executing determination regarding whether or not access can be permitted, based on the screening results in said screening step.

38. An access privilege management method according to Claim 37, wherein said access requested device performs screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group, based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device, and executing determination

regarding whether or not access can be permitted, based on said screening.

39. An access privilege management method according to Claim 37, wherein said access requested device performs screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group, based on a group attribute certificate issued to a user identification device which is an individual identification device at said access requesting device, and executing determination regarding whether or not access can be permitted, based on said screening.

40. An access privilege management method according to Claim 37, further comprising a mutual authentication execution step between security chips with anti-tampering configurations of said access requesting device and said access requested device;

wherein, under the condition that mutual authentication has been established, said access requested device executes signature verification of the group attribute certificate presented from said access requesting device, and screening regarding whether or not the device belongs to an access-permitted group.

41. An access privilege management method according to Claim 37, further comprising a step for said access requested device to receive from a device an issuing request for a group attribute certificate certifying that the device is an access-permitted group member; and

a step wherein, under the conditions that mutual authentication between devices has been established and that the group attribute certificate issue requesting device is following an issuance policy permitted by said access requested device, a group attribute certificate is issued to a device corresponding to a device or a user.

42. An access privilege management method according to Claim 37, further comprising, as an execution step at said access requested device in response to an issuing request from a device for a group attribute certificate certifying that the device is an access-permitted group member, a step for executing processing for issuing a group attribute certificate to a device corresponding to a device or a user, certifying that the device is an access-permitted group member, under the conditions that mutual authentication between devices has been established and that verification and screening is established for an already-issued group attribute certificate already held by the group attribute certificate issue requesting device.

43. An access privilege management method according to Claim 37, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein said access requesting device is of a configuration wherein verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

44. A communication managing method for a communication processing device for executing access restriction processing, said method comprising:

a reception step for receiving, from an access requesting device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer; and

an access privilege determination processing step for executing verification, by means of signature verification, of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering, performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate; and

an access permissible/impermissible determination step for executing determination regarding whether or not access can be permitted, based on the access privilege determination processing results.

45. A communication managing method according to Claim 44, wherein said access privilege determination processing step includes a step performing screening regarding whether or not said access requesting device is an end entity belonging to an access-permitted group, based on a group attribute certificate issued to the end entity which is an access executing device at said access requesting device.

46. A communication managing method according to Claim 44, wherein said access privilege determination processing step includes a step for performing screening regarding whether or not said access requesting device is a device owned by a user belonging to an access-permitted group, based on a group attribute certificate issued to a user identification device which is an individual identification device making up said access requesting device.

47. A communication managing method according to Claim 44, further comprising an authentication processing step for executing mutual authentication with said access requesting device;

wherein, in said access privilege determination processing step, signature verification of the group attribute certificate presented from said access requesting device, and screening regarding whether or not the device belongs to an access-permitted group, are executed, under the condition that mutual authentication has been established.

48. A communication managing method according to Claim 44, wherein said group attribute certificate is of a configuration storing link information regarding a public key certificate corresponding to said group attribute certificate;

and wherein, in said access privilege determination processing step, verification of the public key certificate obtained by said link information is also executed at the time of performing verification of said group attribute certificate.

49. A computer program for effecting execution of a

communication managing method for a communication processing device for executing access restriction processing, said program comprising:

a reception step for receiving, from an access requesting device, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain communication devices or certain users, and also has affixed an electronic signature of an issuer; and

an access privilege determination processing step for executing verification, by means of signature verification, of the group attribute certificate received from said access requesting device regarding whether or not there has been tampering, performing screening regarding whether or not said access requesting device is a device which belongs to an access-permitted group based on group identification information stored in said group attribute certificate; and

an access permissible/impermissible determination step for executing determination regarding whether or not access can be permitted, based on the access privilege determination processing results.

50. A data processing system for executing data processing accompanied by data communication processing, between a plurality of devices capable of mutual

communication, wherein, of said plurality of devices, a data processing requesting device, which requests data processing to the other device with which communication is being made, holds a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer, and transmits said group attribute certificate to a data processing requested device at the time of data processing requesting processing;

and wherein said data processing requested device executes verification processing of the received group attribute certificate, determines whether or not said data processing requesting device has data processing requesting privileges based on said verification, and executes data processing based on determination of privileges.

51. A data processing system according to Claim 50, wherein the group attribute certificate stored in said data processing requesting device has as the issuer thereof the data processing requested device, and has affixed the electronic signature of the data processing requested device;

and wherein said data processing requested device is of a configuration for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate.

52. A data processing system according to Claim 50, wherein all of said mutually communicable plurality of devices are devices which mutually request data processing of the other device with which communication is being made, with each of the devices having a configuration storing the group attribute certificate issued by the communication party device and transmitting the group attribute certificate stored in itself at the time of data processing requesting of the other device with which communication is being made, and under the condition of verification being established at the receiving device, processing corresponding to the data processing request is mutually executed.

53. A data processing system according to Claim 50, wherein all of said mutually communicable plurality of devices have security chips with anti-tampering configurations, with mutual authentication being executed between the mutual security chips at the time of data processing requesting of the other device with which communication is being made, and wherein, under the

condition that mutual authentication has been established, said transmission of group attribute certificates between the devices, and verification of the transmitted group attribute certificates, is executed.

54. A data processing system according to Claim 50, wherein the group attribute certificate stored in the data processing requesting device has as the issuer thereof the data processing requested device;

and wherein issuing processing is performed under the condition that mutual authentication has been established between the data processing requesting device and the data processing requested device.

55. A data processing system according to Claim 50, wherein, of said mutually communicable plurality of devices, at least one or more devices comprise, as a device configuration, an end entity for executing communication processing with other device and data processing, and a user identification device having individual identification functions capable of exchanging data with said end entity;

and wherein, in the event that said group attribute certificate is issued to members making up a certain user group, issuing processing is carried out under the condition that mutual authentication is established between said user identification device and a group attribute certificate issuing processing executing device.

56. A data processing system according to Claim 50, wherein, of said mutually communicable plurality of devices, one is a maintenance executing device for executing maintenance processing for devices;

and wherein the other devices are service receiving device which receive the maintenance service from said maintenance executing device;

and wherein said service receiving device stores a service attribute certificate which is a group attribute certificate issued by said maintenance executing device;

and wherein said maintenance executing device stores a control attribute certificate which is a group attribute certificate issued by said service receiving device;

and wherein said service attribute certificate is applied for verification at said maintenance executing device that said service receiving device belongs to a group of devices or users having maintenance service receiving privileges;

and wherein said control attribute certificate is applied for verification at said service receiving device that said maintenance executing device belongs to a group of devices or users having maintenance service executing privileges.

57. A data processing system according to Claim 56, wherein a maintenance program executed at said service receiving device is transmitted to or stored in said service receiving device as an enciphered maintenance program;

and wherein said service receiving device is of a configuration for deciphering said enciphered maintenance program within a security chip having an anti-tampering configuration, and then executing on said service receiving device.

58. A data processing system according to Claim 56, wherein maintenance processing executed at said service receiving device is executed based on commands transmitted from said maintenance executing device to said service receiving device;

and wherein said service receiving device transmits a response to said maintenance executing device for the execution results of said commands, and said maintenance executing device executes transmission of new commands to said service receiving device based on the transmitted response.

59. A data processing device for executing data

processing based on data processing requests from a data processing requesting device, said data processing device comprising:

a data reception unit for receiving from said data processing requesting device a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer;

a privilege determining processing unit for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification; and

a data processing unit for executing data processing based on determination of privileges.

60. A data processing device according to Claim 59, wherein said privilege determining processing unit is of a configuration for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate.

61. A data processing device according to Claim 59,

wherein said data processing device has a security chip with an anti-tampering configuration and comprising an enciphering processing unit;

and wherein said enciphering processing unit has a configuration wherein mutual authentication is executed with the data processing requesting device in response to a data processing request from the data processing requesting device;

and wherein said privilege determining processing unit is of a configuration for executing verification of the group attribute certificate, under the condition that mutual authentication has been established.

62. A data processing device according to Claim 59, wherein said data processing device is of a configuration comprising an attribute certificate generating processing unit having functions for generating a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature.

63. A data processing method for executing data processing accompanied by data communication processing, between a plurality of devices capable of mutual

communication, wherein, of said plurality of devices, a data processing requesting device, which requests data processing to the other device with which communication is being made, executes a step for transmitting, to the other device with which communication is being made at the time of data processing requesting processing, a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users, and also has affixed an electronic signature of an issuer;

and wherein said data processing requested device executes:

a verification processing step for the received group attribute certificate;

a step for determining whether or not said data processing requesting device has data processing requesting privileges based on said verification; and

a step for executing data processing based on determination of privileges.

64. A data processing method according to Claim 63, wherein the group attribute certificate stored in said data processing requesting device has as the issuer thereof the data processing requested device, and has affixed the electronic signature of the data processing requested

device;

and wherein, in said verification processing step at said data processing requested device, electronic signature verification processing applying a public key of itself is executed, as verification processing of the received group attribute certificate.

65. A data processing method according to Claim 63, wherein all of said mutually communicable plurality of devices are devices which mutually request data processing of the other device with which communication is being made, with each of the devices having a configuration storing the group attribute certificate issued by the communication party device and transmitting the group attribute certificate stored in itself at the time of data processing requesting of the other device with which communication is being made, and under the condition of verification being established at the receiving device, processing corresponding to the data processing request is mutually executed.

66. A data processing method according to Claim 63, wherein all of said mutually communicable plurality of devices have security chips with anti-tampering configurations, with mutual authentication being executed

between the mutual security chips at the time of data processing requesting of the other device with which communication is being made, and wherein, under the condition that mutual authentication has been established, said transmission of group attribute certificates between the devices, and verification of the transmitted group attribute certificates, is executed.

67. A data processing method according to Claim 63, further comprising an issuing processing step for the group attribute certificate stored in the data processing requesting device;

said issuing processing step being executed under the condition that mutual authentication has been established between the data processing requesting device and the data processing requested device.

68. A data processing method according to Claim 63, further comprising an issuing processing step for the group attribute certificate stored in the data processing requesting device;

wherein, in the event that said group attribute certificate is issued to members making up a certain user group, said issuing processing step is executed under the condition that mutual authentication is established with a user identification device having individual identification functions making of the data processing requesting device.

69. A data processing method according to Claim 63, wherein, of said mutually communicable plurality of devices, one is a maintenance executing device for executing maintenance processing for devices, and wherein the other devices are service receiving device which receive the maintenance service from said maintenance executing device, said method comprising:

a step for said service receiving device to transmit to said maintenance executing device a service attribute certificate which is a group attribute certificate issued by said maintenance executing device;

a service attribute certificate verification step for said maintenance executing device to execute verification of the received service attribute certificate;

a step for said maintenance executing device to transmit to said service receiving device a control attribute certificate which is a group attribute certificate issued by said service receiving device;

a control attribute certificate verification step for said service receiving device to execute verification of said control attribute certificate; and

a maintenance processing step for executing maintenance processing under the condition that both verification of said service attribute certificate verification and said control attribute certificate verification have been established.

70. A data processing method according to Claim 69, wherein a maintenance program executed at said service receiving device is transmitted to or stored in said service receiving device as an enciphered maintenance program;

and wherein said service receiving device is of a configuration for deciphering said enciphered maintenance program within a security chip having an anti-tampering configuration, and then executing on said service receiving device.

71. A data processing method according to Claim 69, wherein maintenance processing executed at said service receiving device is executed based on commands transmitted from said maintenance executing device to said service receiving device;

and wherein said service receiving device transmits a response to said maintenance executing device for the execution results of said commands, and said maintenance executing device executes transmission of new commands to said service receiving device based on the transmitted response.

72. A data processing method for executing data processing based on data processing requests from a data processing requesting device, said method comprising:

a data reception step for receiving from said data processing requesting device a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer;

a privilege determining processing step for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification; and

a data processing step for executing data processing based on determination of privileges.

73. A data processing method according to Claim 72, wherein said privilege determining processing step includes a step for executing electronic signature verification processing applying a public key of itself, as verification processing of the received group attribute certificate.

74. A data processing method according to Claim 72, further comprising a step for executing mutual authentication with the data processing requesting device in response to a data processing request from the data processing requesting device;

and wherein said privilege determining processing step executes verification of the group attribute certificate, under the condition that mutual authentication has been established.

75. A computer program for effecting execution of data processing based on data processing requests from a data processing requesting device, said program comprising:

a data reception step for receiving from said data processing requesting device a group attribute certificate which has, as stored information, group identification information corresponding to a group which is a set of certain devices or certain users and also has affixed an electronic signature of an issuer;

a privilege determining processing step for executing verification processing of the received group attribute certificate, and determining whether or not said data processing requesting device has data processing requesting privileges based on said verification; and

a data processing step for executing data processing based on determination of privileges.